UNCLAS

PRECEDENCE TO: ROUTINE DTG: 052157Z MAR 04
PRECEDENCE CC: ROUTINE
TYPE: AUTODIN
FROM PLA: DON CIO WASHINGTON DC
SUBJECT: DON PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION GUIDANCE//
TEXT:
RAAUZYUW RUEWMCS0431 0652157-UUUU--RUENOGC.
ZNR UUUUU ZUI RUENAAA0431 0652157
R 052157Z MAR 04 ZYB
FM DON CIO WASHINGTON DC
TO RUENAAA/ASSTSECNAV FM WASHINGTON DC//00//
RUENAAA/ASSTSECNAV IE WASHINGTON DC//00//
RUENAAA/ASSTSECNAV MRA WASHINGTON DC//00//
RUENAAA/ASSTSECNAV RDA WASHINGTON DC//00//
RUENAAA/AAUSN WASHINGTON DC//00/OPTI//
RUENOGC/OGC WASHINGTON DC//00//
RULSADO/NAVY JAG WASHINGTON DC//00//
RUENAAA/OLA WASHINGTON DC//00//
RUENAAA/CHINFO WASHINGTON DC//00//
RUENAAA/NAVINSGEN WASHINGTON DC//00//
RUENAAA/AUDGEN WNY DC//00//
RULSTGE/NAVCRIMINVSERV WASHINGTON DC//00//
RUENAAA/CNO WASHINGTON DC//N00//
RHMFIUU/CMC WASHINGTON DC//00//
INFO RUENAAA/CNO WASHINGTON DC//N6F//
RHMFIUU/CMC WASHINGTON DC//C4//
RUENAAA/DON CIO WASHINGTON DC//00//
UNCLAS
MSGID/GENADMIN/DON CIO WASHINGTON DC/00/-/MAR//
SUBJ/DON PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION GUIDANCE//
REF/A/DOC/DOD CIO WASHINGTON DC/12JAN2004//
REF/B/DOC/DOD CIO WASHINGTON DC/07OCT2003//
REF/C/MSG/DON CIO WASHINGTON DC/171925ZSEP2003//
REF/D/MSG/DON CIO WASHINGTON DC/031700ZNOV2003//
REF/E/DOC/DOD WASHINGTON DC/24OCT2002//
NARR/REF A ESTABLISHED THE IDENTITY MANAGEMENT SENIOR COORDINATING GROUP (IMSCG). REF B PROMULGATED THE DOD PKI MILESTONES UPDATE. REF C IS THE DON CIO MSG AUTHORIZING A SIX-MONTH EXTENSION UNTIL 01 APRIL 2004 FOR DON COMPLIANCE WITH THE DOD PKI MANDATES. REF D ESTABLISHED PKI IMPLEMENTATION REPORTING GUIDANCE ON PROGRESS TOWARD FULL COMPLIANCE. REF E IS THE DOD INFORMATION ASSURANCE DIRECTIVE.//
POC/LAWRENCE PEMBERTON/CDR USN/DON CIO/LOC:WASHINGTON DC /TEL:703-601-0120//
RMKS/1. REF A ESTABLISHES THE IDENTITY MANAGEMENT SENIOR COORDINATING GROUP (IMSCG) WHICH IS TASKED TO OVERSEE IDENTITY MANAGEMENT WITHIN THE DEPARTMENT OF DEFENSE AND EXPLOIT SYNERGIES IN THE CURRENT COMMON ACCESS CARD, PUBLIC KEY INFRASTRUCTURE, AND BIOMETRICS INITIATIVES. THE DOD CIO SET AS FIRST PRIORITY FOR THIS BODY THE TASK OF IDENTIFYING CURRENT CAPABILITIES AND RECOMMENDING UPDATES TO POLICY AND ASSOCIATED IMPLEMENTATION MILESTONES.
2. PKI IS A FUNDAMENTAL COMPONENT OF OUR NETWORK INFORMATION ASSURANCE STRATEGY AND IS ESSENTIAL IN PROVIDING ENHANCED IDENTITY AUTHENTICATION. THE ENTIRE DON TEAM CONTINUES TO MAKE SIGNIFICANT STRIDES IN FIELDING AND IMPLEMENTING PKI. WE HAVE ISSUED IN EXCESS OF ONE MILLION COMMON ACCESS CARDS WITH PKI CREDENTIALS, ISSUED PKI

SERVER CERTIFICATES TO OUR PRIVATE WEB SERVERS AND CONTINUE TO PK-ENABLE OUR PRIVATE WEB SERVERS FOR CLIENT SIDE AUTHENTICATION.
3. REF B AND REF C SET THE FOLLOWING DOD PKI MILESTONES AT NO LATER THAN 01 APRIL 2004:

A. CLIENT SIDE AUTHENTICATION TO DOD PRIVATE WEB SERVERS

B. DIGITALLY SIGNING ALL E-MAIL SENT WITHIN DOD

C. PK-ENABLE WEB APPLICATIONS IN UNCLASSIFIED ENVIRONMENTS

D. PK-ENABLE DOD UNCLASSIFIED NETWORKS FOR HARDWARE TOKEN CERTIFICATE BASED ACCESS CONTROL

E. DON INDUSTRY PARTNERS OBTAIN DOD PKI DIGITAL CERTIFICATES OR EXTERNAL CERTIFICATE AUTHORITY (ECA) PKI DIGITAL CERTIFICATES.

4. WE CONTINUE TO MAKE GREAT PROGRESS IN THIS COMPLEX ENDEAVOR THAT REQUIRES DOD AS WELL AS DON ACTIONS FOR SUCCESS. SINCE SOME OF THE INFRASTRUCTURE COMPONENTS REQUIRED TO ACHIEVE THE PKI MILESTONES ARE NOT YET COMPLETE, THE DEADLINE WILL BE EXTENDED FOR IMPLEMENTATION OF REF C ACTIONS. WE MUST ALL CONTINUE TO WORK TOWARDS ACHIEVING THESE IMPORTANT MILESTONES, AS SOON AS POSSIBLE. THE FOLLOWING ACTIONS SHALL BE TAKEN IN SUPPORT OF PKI/PKE MILESTONES:

A. CAC/PKI ISSUANCE: ALL DON ORGANIZATIONS SHALL CONTINUE TO ISSUE CACS WITH PKI CERTIFICATES.

B. CAC READER AND MIDDLEWARE DEPLOYMENT: ALL DON ORGANIZATIONS SHALL CONTINUE TO INSTALL CAC READERS AND ASSOCIATED MIDDLEWARE. NMCI, CONUS NON-NMCI, BLII AND MCEN NETWORKS SHALL COMPLETE DEPLOYMENT OF CAC READERS AND MIDDLEWARE BY THE FOLLOWING TIMEFRAMES:

- 50% COMPLETION BY JUN 04
- 75% COMPLETION BY AUG 04
- 100% COMPLETION BY OCT 04

C. CLIENT SIDE AUTHENTICATION TO DOD PRIVATE WEB SERVERS: ALL DON ORGANIZATIONS SHALL CONTINUE TO PK-ENABLE PRIVATE WEB SERVERS AS PLANNED AND TARGET COMPLETION NLT OCT 04. PRIVATE WEB SERVERS THAT HAVE A USER BASE THAT HAS YET TO MIGRATE TO WORKSTATIONS THAT HAVE CAC READERS AND MIDDLEWARE ARE AUTHORIZED TO MAINTAIN CAC BASED AND NON-CAC BASED METHODS OF AUTHENTICATION UNTIL USER BASE HAS MIGRATED OR OCT 04.

D. E-MAIL SIGNING AND ENCRYPTION: AS CAC READERS AND MIDDLEWARE ARE DEPLOYED, DON USERS SHALL DIGITALLY SIGN E-MAIL MESSAGES REQUIRING EITHER MESSAGE INTEGRITY AND/OR NON-REPUDIATION AND ENCRYPT MESSAGES CONTAINING SENSITIVE INFORMATION, AS DEFINED IN REF E ENCLOSURE 2(PARA E2.1.41). E-MAIL THAT IS PERSONAL AND NON-OFFICIAL IN NATURE (E.G., SAILOR MAIL) SHOULD NOT BE DIGITALLY SIGNED.

E. CRYPTOGRAPHIC BASED NETWORK LOGON: NMCI SHALL CONTINUE TO DEPLOY INFRASTRUCTURE COMPONENTS REQUIRED TO SUPPORT THIS CAPABILITY. A DON TIGER TEAM HAS BEEN CHARTERED TO ENSURE THE ACCOMPLISHMENT OF THIS ENDEAVOR. ALL DON ORGANIZATIONS SHALL CONTINUE TO ENABLE ALL NON-NMCI NETWORKS FOR CRYPTOGRAPHIC BASED NETWORK LOGON AS PLANNED AND TARGET COMPLETION NLT OCT 04. WE MUST CONTINUE TO AGGRESSIVELY PURSUE THE SIGNIFICANT SECURITY ENHANCEMENTS ASSOCIATED WITH CRYPTOGRAPHIC BASED NETWORK LOGON.

F. DON INDUSTRY PARTNERS SHALL CONTINUE TO OBTAIN DOD PKI DIGITAL CERTIFICATES OR EXTERNAL CERTIFICATE AUTHORITY (ECA) PKI DIGITAL CERTIFICATES.

5. THIS POLICY WILL BE UPDATED AS REQUIRED. WITH THE EXCEPTION OF THOSE LISTED ABOVE, WE WILL HOLD IN ABEYANCE THE PKI IMPLEMENTATION MILESTONES IN REF C. WE WILL CONTINUE TO WORK ACROSS DOD TO REFINE FUNCTIONAL CAPABILITIES OF THE DOD PKI, DEVELOP A CAPABILITIES EVOLUTION STRATEGY, AND DEVELOP A PKI/PKE IMPLEMENTATION MILESTONE

POLICY THAT IS BETTER ALIGNED WITH THE DOD PKI CAPABILITIES EVOLUTION STRATEGY. THIS CHANGE IN DEADLINES WILL HELP TO ENSURE A REASONABLE IMPLEMENTATION, HOWEVER WE MUST CONTINUE TO AGGRESSIVELY PURSUE CAC AND CERTIFICATE ISSUANCE AND MUST CONTINUE TO AGGRESSIVELY CONTINUE PK-ENABLING ACTIONS.

6. UNTIL FURTHER GUIDANCE IS PROVIDED, ACTION ADDEES SHALL CONTINUE TO PROVIDE DON CIO MONTHLY PKI IMPLEMENTATION STATUS REPORTS PER REF D, AS THEY EVALUATE THEIR RESPECTIVE PKI/PKE IMPLEMENTATION STRATEGIES AND MOVE FORWARD, IN A REASONABLE APPROACH, TOWARDS PK-ENABLING WEB APPLICATIONS AND NETWORKS AND CONDUCT REQUIRED CAC MAINTENANCE ACTIONS AS PKI-BASED CAPABILITIES MATURE AND ARE FIELDED. WE MUST CONTINUE TO MONITOR AND TRACK DON PROGRESS IN REACHING OUR PKI IMPLEMENTATION GOALS.

7. THIS MESSAGE SHOULD NOT BE PERCEIVED AS AUTHORITY TO HALT PROGRESS TOWARDS CONTINUED PKI/PKE ROLLOUT ACTIVITIES. THE DON REMAINS FIRMLY COMMITTED TO ACCOMPLISHING DOD PKI MILESTONES, AS QUICKLY AS IS REASONABLE, IN ORDER TO STRENGTHEN THE SECURITY OF OUR INFORMATION SYSTEMS BY USING PUBLIC KEY TECHNOLOGY AND REALIZE THE BENEFITS OF WEB-BASED SELF SERVICE TRANSACTIONS FOR OUR NAVY-MARINE CORPS TEAM.

8. RELEASED BY D. M. WENNERGREN, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.//

BT

#0431